REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
13-02-2006	FINAL	

4. TITLE AND SUBTITLE

Computer Network Attack and Its Effectiveness against Non-State Actors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Major Timothy D. Presby, U.S. Army

Paper Advisor (if Any): Professor Douglas N. Hime

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Computer Network Attack (CNA) is a subset of Computer Network Operations (CNO), which is a core capability of Information Operations. CNA is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. With the United States engaged in counter-insurgency operations against terrorist groups, synchronizing the effects of CNA with more traditional forms of kinetic attacks, as well as other instruments of national power, permits the United States to achieve its political and military objectives at a reduced cost. The dependency of non-state adversaries on computer systems will only grow as information systems become more pervasive in under-developed nations. CNA, while typically not decisive in itself, can help shape the battlespace and serve as an effective instrument against non-state actors. The effects of CNA can bring synergy, balance, leverage, simultaneity and depth to an operation while helping to achieve the objective in a timely manner with measurable results. Leaders looking to plan and execute CNA operations against non-state opponents need to focus on improved intelligence, better training and awareness, and proper assurance testing and deconfliction to improve the chance of success. Planners also need to be careful to ensure that CNA is conducted within a legal and ethical framework.

15. SUBJECT TERMS

Information Operations, Computer Network Attack, Cyber Warfare, Information Warfare, Non-State Actors, Terrorists, Transnationals, Insurgents, Command and Control, Operational Art

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		22	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, RI

Computer Network Attack and Its Effectiveness against Non-State Actors

By

Timothy D. Presby
Major, U.S. Army

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

13 February 2006

_____
Faculty Advisor
Douglas N. Hime

CONTENTS

ABSTRACT

Computer Network Attack (CNA) is a subset of Computer Network Operations (CNO), which is a core capability of Information Operations. CNA is defined as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves. With the United States engaged in counter-insurgency operations against terrorist groups, synchronizing the effects of CNA with more traditional forms of kinetic attacks, as well as other instruments of national power, permits the United States to achieve its political and military objectives at a reduced cost. The dependency of non-state actors on computer systems will only grow as information systems become more pervasive in under-developed nations. CNA, while typically not decisive in itself, can help shape the battlespace and serve as an effective instrument against non-state adversaries. The effects of CNA can bring synergy, balance, leverage, simultaneity and depth to an operation while helping to achieve the objective in a timely manner with measurable results. Leaders looking to plan and execute CNA operations against non-state opponents need to focus on improved intelligence, better training and awareness, and proper assurance testing and deconfliction to improve the chance of success. Planners also need to be careful to ensure that CNA is conducted within a legal and ethical framework.

INTRODUCTION

JP1-02 defines information superiority as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition."[1] Accordingly, *Joint Vision 2010* states that

> **Information superiority will require both offensive and defensive information warfare (IW). Offensive information warfare** will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers.[2]

Furthermore, *Joint Vision 2020* interjects that "the creation of information superiority is not an end in itself."[3] At the same time the end of the Cold War has created a power shift and a redistribution of authority among states, markets, and society itself.[4] This shift has placed the non-state actor firmly on the world stage. Presently, the United States is engaged in low-intensity operations against terrorist and insurgency groups. Along with these groups, non-state actors and transnational organizations maintain a fundamental reliance at some level on computer and information technology. With continued U.S. hegemony and the potential emergence of another superpower still decades away, similar threats are now more the norm rather than the exception. The purpose of this paper is to examine the effectiveness of information operations (IO), specifically computer network attack (CNA), against non-state adversaries using key facets of operational art as criteria for measuring its success. Synchronizing the effects of CNA with more traditional forms of kinetic attacks, as well as other instruments of national power, permits the United States to achieve its political and

[1] Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Joint Pub 1-02), (Washington, D.C.: 12 April 2001 [As Amended Through 31 August 2005]), 259.
[2] Joint Chiefs of Staff, *Joint Vision 2010*, (Washington, D.C.: July 1996), 16.
[3] Joint Chiefs of Staff, *Joint Vision 2020*, (Washington, D.C.: June 2000), 8.
[4] Jessica T. Mathews, "Power Shift," *Foreign Affairs* 76, no. 1 (January/February 1997): 50.

military objectives at a reduced cost. While there is an extensive body of knowledge about CNA at the classified level, this paper examines the topic strictly from an unclassified viewpoint.

WHAT ARE INFORMATION OPERATIONS AND CNA?

"**'Information operations'** are actions taken to affect adversary information and information systems, while defending one's own information and information systems. IO require the close, continuous integration of offensive and defensive capabilities and activities, as well as effective design, integration, and interaction of C2 with intelligence support. IO are conducted through the integration of many capabilities and related activities. . . . and could include CNA."[5] IO are composed of five principle activities—psychological operations, military deception, operations security, electronic warfare, and computer network operations (CNO). It is within the core capability of CNO that the subdivision CNA is located. CNA is defined "as operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves."[6] While the physical destruction of a computer network or computer system through kinetic means would technically qualify as CNA, the most widespread use of CNA is via the Internet or by physically introducing malicious code into a stand-alone computer system through magnetic or optical media such as a floppy disk or CD-ROM.[7] IO and CNA are conducted across the range of military operations from peacetime deterrence, through crisis management, into the

[5] Joint Chiefs of Staff, *Joint Doctrine for Information Operations* (Joint Pub 3-13), (Washington, D.C.: 9 October 1998), I-9.
[6] Ibid.
[7] "Information Operations: The Hard Reality of Soft Power." Joint Command, Control and Information Warfare School, Joint Forces Staff College, NDU, (2002): 64. http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf. Accessed: November 22, 2005.

full conflict of war. Likewise, IO and CNA are conducted at all three levels of war. While the focus of this paper primarily examines CNA at the operational level, it is important to realize that this distinction is blurred at times due to the inherent nature of computer systems and the likelihood that operations may have to be conducted outside a combatant commander's geographic area of responsibility (AOR). Thus, this reality has led to the decision by the Secretary of Defense to task U.S. Strategic Command (STRATCOM) with the responsibility to integrate and coordinate Department of Defense IO core capabilities that cross geographic AORs. Similarly, non-state and transnational enemies are less likely to adhere to fixed boundaries, which underscores the need to approach this problem from a functional perspective.

VULNERABILITY OF NON-STATE ACTORS

The computer and telecommunications revolution of the past twenty years has given rise to the non-state actor on a global level and has precipitated the decline of the non-state actor's reliance on nation-states. "Widely accessible and affordable technology has broken governments' monopoly on the collection and management of large amounts of information and deprived governments of the deference they enjoyed because of it."[8] New technologies, which include laptop computers with their wireless Internet connectivity, substantially reduce the importance of proximity, permitting like-minded non-state adversaries to communicate and coordinate their efforts with relative ease, thus enabling scattered identities from around the world to join together and thrive.[9] It is this reliance on technology and information exchange that needs to be exploited by the United States and her allies to target effectively an

[8] Mathews, 51.
[9] Ibid., 52.

empowered enemy. Non-state enemies and, specifically, terrorists use the Internet in a variety of ways, which include, but are not limited to command and control, as an information/media instrument and as a recruiting or financial tool.

The Internet serves as both a forum for propaganda and a conduit for these organizations to communicate. "At least 12 of the 30 groups on the State Department's list of designated foreign terrorist organizations maintain Web sites on the Internet."[10] Mohammed Mansour Jabarah, a captured al Qaeda terrorist, explained in his confession to U.S. authorities describing how he used e-mail to plan and coordinate an attack against a Bali nightclub in Indonesia in October 2002. Jabarah further described how he used an e-mail account provided from a free Internet mail service provider to maintain communications with Khalid Sheikh Mohammed, a chief organizer of the September 11 attacks in New York.[11] This episode illustrates how like-minded terrorists, lacking geographic proximity, can leverage information technology to communicate and coordinate their efforts effectively.

Non-state adversaries are also looking to the Internet and other information technologies as tools to raise both awareness for their causes and as a means to raise monetary support. A relatively quick and inexpensive method to preach their propaganda to the masses is through websites. Not only are these websites a mechanism to deliver a message to their followers, but they can also serve as a potential recruitment tool. The ability of mainstream media to re-broadcast and amplify the contents of these websites through more traditional means only advances the distribution of their message, while providing a certain level of legitimacy to the organization. With regard to using the Internet for fund-raising purposes,

---

[10] "Terrorist Activities on the Internet." (Winter 1998). http://www.adl.org/terror/focus/16_focus_a.asp. Accessed: January 06, 2006.
[11] Rich Sheehan, "Exploiting Our Asymmetric Technical Advantage to Enhance National Security." SANS Institute (2003): 7. http://www.sans.org/rr/special/NIALV/paper.php?id=sheehan. Accessed: January 06, 2006.

terrorist organizations such as al Qaeda have used Islamic charitable organizations to solicit funding for jihad against enemies of Islam. On multiple occasions investigators have linked bank account numbers and information to both humanitarian relief organizations and known al Qaeda operatives. Furthermore, web portals specializing in the anonymous transfer of funds are readily available to terrorist groups.[12] Through these examples one can see that the Internet can serve as an essential conduit for non-state enemies and terrorist organizations in securing critical financial support. Moreover, the means by which these organizations acquire money through the web can be both legitimate and deceptive. Key to all these activities is the anonymity that computer systems provide. A variety of encryption methods are widely employed to deceive and mask these organizations' true intentions. Techniques such as steganography, the science of placing encrypted messages within another electronic file, are widely used. "A recent government report indicated that terrorists have been hiding pictures and maps of targets in sports chat rooms, on pornographic bulletin boards and on Web sites."[13] Although the goal of the United States is to disrupt, deny, degrade, or destroy these efforts, the enemy is taking active measures to reduce his susceptibility.

DESIRED EFFECTS OF CNA

Colonel Mark Rayfield, deputy commander of the Joint Information Operations Center, Lackland AFB, Texas declared, "with the terrorist threat, we're not necessarily trying to counter the actions of a nation-state. These terrorist organizations use existing commercial processes—whether it's financial or shipping or logistics processes—that the civilian world

[12] Timothy L. Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'." *Parameters* 33, no. 1 (Spring 2003): 115-116.
[13] Jay Lyman, "How Terrorists Use the Internet." NewsFactor Network. (12 September 2001). http://www.newsfactor.com/perl/story/7731.html. Accessed: January 06, 2006.

uses and could have an impact worldwide."[14] As the United States engages in combat operations it must continue to integrate less conventional, non-kinetic forms of attack in conjunction with more traditional forms of attack to shape the battlespace and achieve the desired effects. Before the desired effects of CNA can be discussed in detail, an understanding of the two broad categories of computer networks is required. The first category is an information system, which includes databases, documents, web pages, and e-mail. In contrast, the second broad type of information system is an infrastructure-control system, which could include power, chemical, or water plants, integrated air defense systems, and robots on a manufacturing line.[15] While the effect of attacking an information system is usually aimed at a human decision maker, the effect of attacking an infrastructure-control system is more conventional because the desired effect is to disable or destroy a physical object. As discussed in the previous section, non-state adversaries and terrorists are heavily reliant on information systems, so while the intended target of CNA is an information system, the ultimate effect is directed at people. Dr. Dan Kuehl, a professor and leading advocate of IO at the National Defense University stated, "The ultimate objective must be focused on the human. It might be a decision maker, but it might also be 5 million inhabitants of a country. . . . You are doing things to hardware and software networks as a means of influencing humans."[16]

Another way to study the intended effects of CNA is to examine it in terms of levels of war. Contemporary military theory divides war into three levels: tactical, operational, and

---

[14] Maryann Lawlor, "Information Operations Specialists Move to Mission Planners' Table." *Signal* 60, no. 4 (December 2005): 49.
[15] Tim Gibson, "What You Should Know about Attacking Computer Networks." *United States Naval Institute Proceedings* 129, no. 1 (January 2003): 48-49.
[16] Dan Kuhel, "Information Operations Interview with Professor Dan Kuehl." Interview by Wanja Eric Naef (London July 2003). *Infocon Magazine* no. 1 (October 2003): 2. http://www.iwar.org.uk/infocon/io-kuehl.htm. Accessed: November 22, 2005.

strategic. The tactical level translates potential combat power into success in battles and engagements that support a campaign or major operation through the ordered arrangement and maneuver of combat forces. The operational level of war is concerned with using military forces in a theater of operations to obtain an advantage over the enemy through the design, organization, and conduct of major operations by linking tactical achievements into strategic success. The strategic level focuses on supporting national policy and relates directly to the outcome of a war.

CNA can support tactical combat operations, which might include the suppression of enemy air defense (SEAD), psychological or military deception operations.[17] While SEAD is less relevant to the non-state opponent and probably not appropriate for the application of CNA, both psychological and military deception operations could augment and shape a larger operation or campaign. Additionally, these operations could expand and be useful at the operational level of war. The ability to disrupt web operations could affect the non-state adversary's ability to promote himself, thus affecting his ability to recruit and leading to the interruption of his financial operations. While these operations could be shifted to other platforms or computer systems, the disruption of their computer-related activities would give pause to transnational groups to re-evaluate the security of their processes. Also at the operational level of war, CNA could support forward presence operations, support contingency operations, or serve as a deterrent.[18] A combatant commander can use CNA to degrade a terrorist's ability to communicate and coordinate. As was previously mentioned, recent advances in information technology have empowered geographically separated terrorist

[17] "Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat." AUSA Background Brief, Institute of Land Warfare Publication no. 96. (November 2002): 2-3.
[18] "Computer Network Operations—An Integral Part of Land Force Operations." AUSA Background Brief, Institute of Land Warfare Publication no. 93. (December 2001): 2.

groups. The inherent dependency on computer systems for effective command and control makes non-state actors even more vulnerable and keeps them off balance by forcing them to relocate their operations. CNA could also be useful at the strategic level. As an element of a comprehensive IO campaign, CNA could display U.S. resolve to maintain and uphold certain human rights or democratic ideals.[19] While strategic consequences are possible, CNA is much more likely to be successful as part of an integrated IO campaign at the operational level because it can influence and persuade an operational-level decision-maker who relies heavily on computer and information systems. Finally, CNA can support defensive information operations through the concept of active defense, that is, attacking an enemy's computer or information system that might be used to attack or exploit friendly computer systems and networks.[20] While it is apparent that the target of CNA is the information and computer systems used by our adversaries, it is important not to forget that the desired effect is directed against human decision-makers at all levels of war.

ANALYSIS IN TERMS OF OPERATIONAL ART

The effectiveness of CNA is measured in a variety of ways by the attacker in order to determine whether the activities being conducted are having the desired effect as they relate to the overall mission and objective. General criteria for measuring the effectiveness of CNA should include the following—relation to the objective, measurable results, and timeliness.[21] Additionally, the author feels that certain facets of operational art are relevant in analyzing the effectiveness of CNA and has chosen to include synergy, balance, leverage, simultaneity and

[19] Ibid.
[20] "Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat," 3.
[21] Joint Chiefs of Staff, *Information Operations* (Joint Pub 3-13). Revision Final Coordination, (Washington, D.C.: 5 July 2005), V-28 - V-30.

depth in this qualitative analysis. While it can be hard to isolate events and ascertain a direct cause-effect relationship between CNA actions and measured effects, the criteria I have selected serves as a good benchmark from which to measure the usefulness of CNA against non-state enemies.[22]

Objective. As with any form of attack including CNA, a clear objective should be determined before commencing operations. JP1-02 defines objective as "clearly defined, decisive, and attainable goals towards which every military operation should be directed."[23] Dissecting the objective into its three core elements: defined, decisive, and attainable provides a good indication to its application to CNA and its use against non-state adversaries. CNA operations must be clearly defined before being executed; that is, is the attack focused on a command and control capability like email or is it directed against a recruitment or propaganda tool like a website? Next, can CNA be decisive? This is a far more difficult effect to evaluate. Unlike a CNA attack against a nation-state, where actions may focus to compromise or defeat an infrastructure-control system, the primary target in a CNA attack against a terrorist group or non-state opponent is a human audience and the decisions they make. So, while it is argued that CNA can be complementary in its battlespace shaping effects, it is less likely to be decisive by itself against a non-state enemy. Finally, is CNA a realistic and attainable option for an operational commander? This goal is more problematic when targeted against a non-state adversary. Because non-state opponents lack a readily exploitable fixed infrastructure, the challenge lies in one's ability to target effectively the computer and information systems in use by terrorist organizations and non-state enemies. To ensure that the right target is selected so that the appropriate effect is achieved, a robust

[22] Ibid., V-31.
[23] Joint Pub 1-02, 383.

intelligence mechanism must be focused on the problem of finding and fixing the appropriate computer or information system. While there are unmistakabe challenges inherent with the effective use of CNA against non-state adversaries, a defined, decisive, and attainable goal is possible.

Measurable Results. Ideally, results of the CNA attack, both against the computer systems and the human decision-maker, should be measurable both quantitatively and qualitatively. Prior to measuring the effectiveness, a baseline should be established to accurately capture the effects for a valid comparison.[24] Quantitative measurements are typically easier to gauge. As an example, it is far easier to capture the number of computer intrusions into a system than it is to qualitatively analyze the effects of CNA on a population or a decision-maker. In a more challenging example, media analysts familiar with the targeted population that the non-state opponent is trying to influence could examine the results of CNA's use against recruitment websites and provide an evaluation. To assist in the assessment of the effectiveness of CNA, access to an enemy's internal reporting of the attack would be useful to determine how the adversary responds to the attack and the countermeasures he implements. Compounding the problem, the adversary will most likely implement active defensive measures to limit the attack itself, as well as any follow-up assessments of the attack. More traditional forms of intelligence collection could provide key indicators as to the effect that CNA might have on any financial or logistic system that the non-state enemy uses. Measurable results are possible with respect to the use of CNA, but the key challenge is separating the effects of other forms of IO, as well as more traditional kinetic attacks to determine the true impact of CNA.

[24] Joint Pub 3-13, Revision Final Coordination, V-29.

Timeliness. A key goal for all operations is that they be conducted in a timely manner to ensure that initiative and momentum are maintained. Measuring the effectiveness of CNA operations may require rapid feedback in an effort to remain inside an adversary's decision cycle. With respect to CNA and a non-state opponent's lack of computer infrastructure, it is essential that CNA and its assessment be conducted in an expeditious manner to ensure the desired effect is achieved; that is, the decision-maker is influenced in such a way that he modifies or changes his operations. If a terrorist group suspects the computer system they are using is compromised, they will likely change systems and could change the manner in which they conduct their operations. The impact of such a change could have profound effects and would require a substantial reinvestment of intelligence resources to achieve the preconditions necessary to make CNA possible. As an example, a terrorist group is attempting to influence public sentiment through the use of an inflammatory website. In this case, a narrow window of opportunity exists for CNA to be used effectively. Despite these restrictions, when correctly used and with the proper intelligence assets capable of selecting the proper targets, CNA can serve as a valuable and timely option against non-state adversaries.

Synergy. A goal of any operation is to synchronize and integrate actions across both time and space, culminating in achieving the objective as quickly as possible. Both symmetric and asymmetric actions are executed in order to capitalize on friendly strengths and exploit an enemy's weakness.[25] CNA can provide some unique asymmetrical advantages when combating a non-state actor. By virtue of their dispersed nature, non-state actors have a susceptible dependency on computer systems since they rely heavily on these systems to conduct command and control. As an illustration, a geographically dispersed terrorist

[25] Joint Chiefs of Staff, *Doctrine for Joint Operations* (Joint Pub 3-0), (Washington, D.C.: 10 September 2001), III-9.

network may use a website to post critical information regarding future operations. With the proper intelligence resources that can confirm the authenticity and use of the website, CNA could be used to deny access to the website temporarily, thus delaying intended terrorist operations, and permitting other forms of IO or other dimensions of combat power like firepower and maneuver to be employed. So, while not necessarily decisive in itself, CNA can augment these other operations to achieve an operation's objective.

Balance. "**Balance is the maintenance of the force**, its capabilities, and its operations in such a manner as to **contribute to freedom of action and responsiveness**."[26] While friendly forces attempt to preserve a balance of their capabilities across all dimensions of combat power, IO and, specifically, CNA is an ideal tool to disrupt an adversarial non-state opponent's balance by unexpectedly attacking crucial vulnerabilities. Financing operations are a key aspect of any organization, and while more traditional instruments of national power, like economic sanctions or embargoes, might be effective against a conventional nation-state over a period of several years, it is far more difficult to apply these techniques against a non-state adversary. Nevertheless, there is a certain reliance by non-state enemies on computer and information systems to solicit, move, and disburse funds. In conjunction with more traditional economic forms of power, CNA can effectively disrupt or deny critical financial transactions and could be leveraged as an intelligence gathering tool to identify funding sources and expenditures that could be exploited further by other means.

Leverage. Achieving, preserving, and exploiting advantages across all aspects of combat power characterize leverage.[27] CNA must capitalize on its asymmetric advantages against a non-state adversary throughout the operational factors of space and time to provide a

[26] Ibid., III-13.
[27] Ibid., III-14.

decisive advantage. The uncertainty that CNA brings to bear upon an opponent can influence his entire decision-making process, causing the terrorist leaders to make illogical choices that are vulnerable to exploitation. In this manner CNA can also serve as a deterrent prior to the commencement of hostilities by causing a terrorist leader to delay or modify his actions in a counterproductive fashion. Thus, CNA allows a commander to leverage other forces and capabilities to accomplish his desired objective.

Simultaneity and Depth. Synchronizing operations continuously throughout time and space can produce devastating results against an adversary. The enemy's ability to make rational decisions is negatively impacted by these overwhelming and synchronized operations. CNA contributes to this irrational decision-making by generating confusion and uncertainty in the enemy's actions. Additionally, CNA can be applied at all levels of war. Actions initiated at the tactical level could have effects at the operational or possibly at the strategic level. CNA could be planned at the tactical level as part of a psychological operation to support a tactical engagement, but the resultant effect might cause hesitancy in terrorist leaders that lead to operational mistakes. An example of this indecisiveness might be accelerating the timeline for a bombing. The hastened bombing might result in reduced or unintended casualties; that is, a greater number of locals, whom the non-state opponent is trying to influence positively, are killed. While not vital in itself, CNA can be effective in both simultaneity and depth to attain the desired outcome against a non-state actor.

CHALLENGES AND RECOMMENDATIONS

There remain several challenges that must be overcome to increase CNA's effectiveness and realize its full potential against non-state adversaries. After careful review,

three recommendations are proposed: improved intelligence, better training and awareness, and proper assurance testing and deconfliction. An additional challenge, however, accompanying these recommendations, is that CNA must be conducted within an established legal and ethical framework. Collectively, these recommendations can help improve the effectiveness of CNA and make it a more potent weapon against non-state actors.

Improved Intelligence. A common theme that permeates most of this analysis is the need for proper intelligence applied throughout all phases of CNA. From the initial phases of targeting through to the final phases of battle damage assessment, it is crucial that the appropriate intelligence assets are properly resourced for this task. These assets could vary widely depending on the specific type of operation, but may include human intelligence, signals intelligence, or electronics intelligence. Unfortunately, current collection and intelligence methods were designed to support more conventional kinetic attacks. While improvements are being made in the intelligence field to address these shortcomings, it is imperative that intelligence capabilities related to non-traditional forms of warfare, like CNA, be properly prioritized and resourced. The intelligence process must also be accelerated to maximize the synergy and leverage that CNA brings to the fight. For CNA to be effective, a rapid and robust intelligence mechanism must be implemented to provide the timely feedback necessary to ensure the objectives are met. Steps are being taken in the right direction with STRATCOM developing a joint integrative analysis and planning capability (JIAPC) to provide targeting, planning, and analysis in a timely manner in support of combatant commander IO requirements, but continuing funding difficulties and the complexities of interagency coordination will continue to make improved intelligence a challenge.[28]

[28] Christopher Lamb, "Information Operations as a Core Competency." *Joint Force Quarterly* no. 36 (December 2004): 94.

Better Training and Awareness. Enhanced training and awareness go hand in hand. As an IO core capability, CNA is still in its infancy. The proliferation and advancement of computer systems in the last decade alone indicate that CNA has not reached maturity. The skill set required to conduct CNA is both wide-ranging and highly perishable. As new hardware and software platforms emerge, operators must be more diligent and creative in their efforts to exploit these systems. Compounding the problem is the lack of fixed infrastructure inherent to the non-state enemies and terrorist groups. While Joint Task Force–Computer Network Operations (JTF–CNO) is taking active measures to ensure that a highly capable and professional force is prepared to conduct CNA, the changing complexities of the discipline, which include new software operating systems, new hardware platforms, and emerging networking protocols, require increased attention and effort.

Increased awareness by the operational commander is another aspect of CNA that needs to be addressed. The apparent lack of CNA can be credited to the fact that many senior leaders are unaware of CNA's capabilities. Familiar with the available arsenal of kinetic weapons, they are unlikely to employ CNA unless they are educated about the potential effects of this weapon. Similarly, if CNA planning is kept compartmentalized, it is improbable that in time of crisis its use will be approved. IO capabilities, and especially CNA, must not only be taught, but must be emphasized at all educational levels. Only after senior leaders gain a thorough understanding of CNA will its potential be fully realized.[29]

Proper Assurance Testing and Deconfliction. To minimize the likelihood of collateral damage, assurance testing is crucial. Assurance testing is a qualitative control measure designed to assess the expected outcome over a series of trials in an effort to accomplish the task with a minimal amount of unintentional consequences. Constant

[29] "Information Operations: The Hard Reality of Soft Power," 66.

hardware upgrades and software updates complicate CNA and increase the possibility that operations may have unintended effects. Systematic and methodical assurance testing needs to be conducted to ensure that the anticipated outcome is achieved. Although I advocate thorough testing, exhaustive and conclusive results may not be possible within the desired timeframe of the individual operation, leaving the commander to balance the risk-reward aspect of CNA. Both automated and manual processes need to be developed to expedite assurance testing so that CNA can be executed in both a reliable and timely manner. The Department of Defense may not be the only activity engaging in CNA. While Title 10 responsibilities limit the extent to which the military may conduct CNA, other organizations within the U.S. government or among coalition partners may be planning and executing their own CNA operations. The transnational aspect of twenty-first century non-state adversaries may make deconfliction even more difficult due to the dispersed global nature of their organizations. Thorough deconfliction within the U.S. government and with our allies is required to ensure that the intended effects of CNA are realized.

Legal and Ethical Framework. A pervasive challenge to the use of CNA against a non-state opponent is the ability for the user of CNA to remain within the legal and ethical boundaries of warfare. Computer networks can be transient in nature and the fact that non-state adversaries and terrorist groups will operate computer and information systems within multiple nation-states only further clouds the legal landscape. The unease over NATO's use of CNA against Yugoslavia in 1999 is convincing proof that the problem of how humanitarian law applies to CNA is uncertain.[30] While the use of CNA should follow the general legal guidelines of being discriminate and proportional in nature, the effects of CNA

[30] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and *jus in bello*." *International Review of the Red Cross* 84, no. 846 (June 2002): 396.

may cause unintended consequences that require special consideration during both the planning and execution phase of operations. From an ethical standpoint, the situation is equally unclear. While CNA is obviously an act of force, CNA by itself is not morally wrong. Its moral connotation originates from the circumstances of its use, particularly the manner of attack and the target.[31] While the use of CNA against non-state enemies can be both legal and ethical in nature, legal experts need to participate fully in the planning and execution of CNA operations to ensure that legitimacy is maintained.

CONCLUSION

With the United States engaged in counter-insurgency operations against terrorist groups, synchronizing the effects of CNA with more traditional forms of kinetic attacks, as well as other instruments of national power, permits the United States to achieve its political and military objectives at a reduced cost. The dependency of non-state actors on computer systems will only grow as information systems become more pervasive in under-developed nations. CNA, while typically not decisive in itself, can help shape the battlespace and serve as an effective instrument against non-state adversaires. The effects of CNA can bring synergy, balance, leverage, simultaneity and depth to an operation while helping to achieve the objective in a timely manner with measurable results. Military leaders looking to plan and execute CNA operations against non-state opponents need to focus on improved intelligence, better training and awareness, and proper assurance testing and deconfliction to improve the chance of success. Planners also need to be careful to ensure that CNA is conducted within a legal and ethical framework.

[31] William J. Bayles, "The Ethics of Computer Network Attack." *Parameters* 31, no. 1 (Spring 2001): 55.

SELECTED BIBLIOGRAPHY

Bayles, William J. "The Ethics of Computer Network Attack." *Parameters* 31, no. 1 (Spring 2001): 44-58.

"Computer Network Operations: A Critical Element of Current and Future Military Operations in Combating the Asymmetrical Threat." AUSA Background Brief, *Institute of Land Warfare Publication* no. 96. (November 2002): 1-6.

"Computer Network Operations—An Integral Part of Land Force Operations." AUSA Background Brief, *Institute of Land Warfare Publication* no. 93. (December 2001): 1-4.

Department of the Army. *Information Operations: Doctrine, Tactics, Techniques, and Procedures* (U.S. Army Field Manual 3-13). Washington, D.C.: November 2003.

Gibson, Tim. "What You Should Know about Attacking Computer Networks." *United States Naval Institute Proceedings* 129, no. 1 (January 2003): 48-51.

"Information Operations: The Hard Reality of Soft Power." Joint Command, Control and Information Warfare School, Joint Forces Staff College, NDU, (2002). http://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf. Accessed: November 22, 2005.

Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms* (Joint Pub 1-02). Washington, D.C.: 12 April 2001 (As Amended Through 31 August 2005).

_____. *Doctrine for Joint Operations* (Joint Pub 3-0). Washington, D.C.: 10 September 2001.

_____. *Information Operations* (Joint Pub 3-13). Revision Final Coordination. Washington, D.C.: 5 July 2005.

_____. *Joint Doctrine for Information Operations* (Joint Pub 3-13). Washington, D.C.: 9 October 1998.

_____. *Joint Vision 2010*. Washington, D.C.: July 1996.

_____. *Joint Vision 2020*. Washington, D.C.: June 2000.

Kuhel, Dan. "Information Operations Interview with Professor Dan Kuehl." Interview by Wanja Eric Naef (London July 2003). *Infocon Magazine* no. 1 (October 2003): 1-6. http://www.iwar.org.uk/infocon/io-kuehl.htm. Accessed: November 22, 2005.

Lamb, Christopher. "Information Operations as a Core Competency." *Joint Force Quarterly* no. 36 (December 2004): 88-96.

Lawlor, Maryann. "Information Operations Specialists Move to Mission Planners' Table." *Signal* 60, no. 4 (December 2005): 47-50.

Lenderman, Curtis C. "Computer Network Attack: An Operational Tool?" Unpublished Research Paper, U.S. Naval War College, Newport, RI (17 January 2003): 1-21.

Lyman, Jay. "How Terrorists Use the Internet." NewsFactor Network. (12 September 2001). http://www.newsfactor.com/perl/story/7731.html. Accessed: January 06, 2006.

Mathews, Jessica T. "Power Shift." *Foreign Affairs* 76, no. 1 (January/February 1997): 50-66.

Schmitt, Michael N. "Wired Warfare: Computer Network Attack and *jus in bello*." *International Review of the Red Cross* 84, no. 846 (June 2002): 365-399.

Sheehan, Rich. "Exploiting Our Asymmetric Technical Advantage to Enhance National Security." SANS Institute (2003): 1-21 http://www.sans.org/rr/special/NIALV/paper.php?id=sheehan. Accessed: January 06, 2006.

"Terrorist Activities on the Internet." (Winter 1998). http://www.adl.org/terror/focus/16_focus_a.asp. Accessed: January 06, 2006.

Thomas, Timothy L. "Al Qaeda and the Internet: The Danger of 'Cyberplanning'." *Parameters* 33, no. 1 (Spring 2003): 112-123.